IN THE CLAIMS:

Please amend the claims as indicated. A complete set of the claims is included below, reflecting added subject matter *(underlining)* and deleted subject matter *(strikethrough)*, as well as the current status of each claim. This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for controlling access to an object in an operating system, the method comprising:

receiving a call from an external object to a first interface of a target object;

at the target object, the target object determining whether the external object has access to other interfaces of the target object based on the call to the first interface;

wherein the determining step comprising examining a security policy contained entirely within the target object and purely determined by the first interface; and

granting access to the other interfaces according to the determination.

2-3. (Cancelled)

4. (Previously Presented) A method as recited in claim 1, further comprising determining whether the external object and the target object operate in a same process.

5. (Previously Presented) A method as recited in claim 1, wherein determining whether the external object has access to the other interfaces of the target object further comprises:

identifying the other interfaces of the target object that can be accessed when the first interface is being requested by the external object.

6. (Original) A method as recited in claim 1, further comprising determining a first process of the target object.

7. (Original) A method as recited in claim 6, further comprising determining a second process of the external object.

8. (Original) A method as recited in claim 7, further comprising performing a cross-process communication between the target object and the external object.

9. (Original) A method as recited in claim 1, further comprising securing a channel for each interface of the target object.

10. (Previously Presented) A method as recited in claim 1, wherein determining whether the external object has access to the other interfaces of the target object further comprises analyzing access constraints within the target object.

11. (Original) A method as recited in claim 1, further comprising analyzing interface access data stored within the target object.

12. (Original) A method as recited in claim 1, further comprising determining whether the target object and the external object are in a same protection domain.

13. (Original) A method as recited in claim 12, wherein the protection domain is a process.

14. (Previously Presented) A method as recited in claim 1, wherein the target object sets the target object's own security policy.

15. (Previously Presented) A method as recited in claim 1, wherein determining whether the external object has access to the other interfaces further comprises determining capabilities of the external object.

16. (Previously Presented) A method as recited in claim 15, further comprising mapping the capabilities of the external object to the interfaces of the target object.

17. (Previously Presented) A method as recited in claim 1, wherein the target object and the external object are created using a same methodology.

18. (Previously Presented) A method as recited in claim 1, wherein the target object and the external object are views in a view hierarchy.

19. (Previously Presented) A method as recited in claim 18, wherein a view has a parent calling interface, a child calling interface, and a child managing interface.

20. (Currently Amended) A system that controls access to an object in an operating system, the system comprising:

a module configured to receive a call from an external object to a first interface of a target object;

a module configured to determine at the target object whether the external object has access to other interfaces of the target object based on the call received at the first interface, the determination including examining a security policy contained entirely within the target object and purely based on the first interface; and

a module configured to grant access to the other interfaces according to the determination.

21. (Currently Amended) A system that controls access to an object in an operating system, the system comprising:

means for receiving a call from an external object to a first interface of a target object;

means for determining, at the target object and by the target object, whether the external object has access to other interfaces of the target object based on the call to the first interface;

means for examining a security policy contained entirely within the target object and purely based on the first interface; and

means for granting access to the other interfaces according to the determination.

22-30. (Canceled)

31. (Currently Amended) A computer readable storage medium storing instructions for controlling a computer device to control access to an object in an operating system, the instructions comprising:

receiving a call from an external object to a first interface of a target object;

at the target object, determining whether the external object has access to other interfaces of the target object based on the call to the first interface, the determining step comprising examining a security policy contained entirely within the target object and purely based on the first interface; and

granting access to the other interfaces according to the determination.

32. (Withdrawn) A method as recited in claim 1, further comprising the step of securing the object in the operating system, utilizing the steps of:

determining one or more access constraints of the target object;

identifying a protection domain that has a security profile that corresponds to the one or more access constraints of the target object; and

placing the target object in the protection domain.

33. (Withdrawn) A method as recited in claim 32, further comprising the step of:

creating the target object and a second object using the same methodology.

34. (Withdrawn) A method as recited in claim 33, wherein the target object and the second object can communicate transparently across two or more protection domains.

35. (Withdrawn) A method as recited in claim 32, wherein the protection domain is a process.

36. (Withdrawn) A method as recited in claim 32, further comprising the step of:

creating an object-to-object security model wherein security constraints for an object are contained within the object.

37. (Withdrawn) A method as recited in claim 32, wherein identifying a protection domain further comprises attempting to identify a protection domain that is local relative to the target object.

38. (Withdrawn) A method as recited in claim 32, further comprising the step of:

creating a process based on security requirements of the operating system.

39. (Withdrawn) A method as recited in claim 38, further comprising the step of:

clustering objects in the process based on security policies of the objects.

40. (Withdrawn) A system as recited in claim 21, further comprising a system for securing the object in the operating program, the system comprising:

means for determining one or more access constraints of the target object;

means for identifying a protection domain that has a security profile that corresponds to the one or more access constraints of the target object; and

means for placing the target object in the protection domain.